AMENDMENTS TO THE CLAIMS

Applicant amends claims 24, 26, 27, 39-41, 43, and 44 as indicated below. This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1.-23. (Canceled)

24. (Currently Amended) A method for the cipher controlled exploitation of data resources stored in a remote database associated with a computer system, comprising the steps of:

providing a subscriber identity module carrying at least one security algorithm, said subscriber identity module not used by said computer system for communication with a network;

producing a cipher key via said at least one security algorithm;

using said cipher key for protecting said data resources; and

storing said protected data resources in said remote database in an encrypted format ~~along with said data resources~~.

25. (Previously Presented) The method according to claim 24, wherein said step of using said cipher key for protecting said data resources comprises the steps of:

encrypting said data resources by means of said cipher key;

storing said encrypted data resources in said remote database associated with said computer system;

retrieving said encrypted data resources from said remote database; and decrypting said encrypted data resources by means of said cipher key.

26. (Currently Amended) The method according to claim 24, wherein said step of producing a cipher key comprises the steps of:

generating at least one random value;

subjecting said at least one random value to said at least one security algorithm to generate at least one session key; and

processing said at least one session key via a mixer function to produce said ~~at least one~~ cipher key.

27. (Currently Amended) The method according to claim 26, comprising the steps of:

generating at least two random values;

subjecting said at least two random values to said at least one security algorithm to generate at least two session keys; and

combining said at least two session keys via a mixer function to produce said ~~at least one~~ cipher key.

28. (Previously Presented) The method according to claim 26, wherein said mixer function comprises a hash function.

29. (Previously Presented) The method according to claim 26, comprising the step of inserting in said mixer function a user specific secret unrelated to said subscriber identity module security algorithm, whereby said cipher key is unpredictable even based on knowledge of said security algorithm carried in said subscriber identity module.

30. (Previously Presented) The method according to claim 24, comprising the step of selecting said data resources from user sensitive data or user credentials.

31. (Previously Presented) The method according to claim 30, wherein said step of using said cipher key for protecting said data resources comprises the step of encrypting by means of said cipher key, said user sensitive data or said user credentials from plain text into an encrypted format.

32. (Previously Presented) The method according to claim 31, wherein said step of using said cipher key for protecting said data resources comprises the step of decrypting by means of said cipher key said user sensitive data or said user credentials from an encrypted format into plain text.

33. (Previously Presented) The method according to claim 31, wherein said user sensitive data or said user credentials in encrypted format have a cryptographic header associated therewith.

34. (Previously Presented) The method according to claim 33, wherein said cryptographic header comprises an identifier of said subscriber identity module and a cryptographic checksum based on said cipher key, said cryptographic checksum being used for detecting any unauthorized modifications of said encrypted format.

35. (Previously Presented) The method according to claim 30, wherein said data resources are user credentials and said data resources based on said user credentials are stored in said remote database in an encrypted format.

36. (Previously Presented) The method according to claim 35, comprising the step of establishing a relationship between said user credentials stored in said encrypted format in said remote database and a corresponding user subscriber identity module.

37. (Previously Presented) The method according to claim 36, wherein said relationship is established by means of an identifier of said subscriber identity module.

38. (Previously Presented) The method according to claim 37, comprising the step of using said identifier for searching within said remote database to permit [[said]] user exploitation of said user credentials.

39. (Currently Amended) A system for cipher-controlled exploitation of data resources, comprising:

at least [[a]] one subscriber identity module carrying at least one security algorithm;

at least [[a]] one computer system comprising at least one processing module, said subscriber identity module not used by said at least one computer system for communication with a network and said at least one processing module being interfaced with said at least one subscriber identity module to generate ~~at least one~~ a cipher key via said at least one security algorithm and being configured to protect via said cipher key said data resources; and

a remote database associated with said at least one computer system for storing said ~~data resources and~~ protected data resources by said cipher key in an encrypted format.

40. (Currently Amended) The system according to claim 39, wherein said at least one processing module is configured for:

encrypting said data resources by means of said cipher key;

storing said encrypted data resources in said remote database associated with said at least one computer system;

retrieving said encrypted data resources from said remote database; and decrypting said encrypted data resources by means of said cipher key.

41. (Currently Amended) The system according to claim 39, wherein said remote database is included in said at least one computer system.

42. (Canceled)

43. (Currently Amended) The system according to claim 39, wherein said at least one processing module is interfaced with said at least one subscriber identity module via a smart card reader or a Bluetooth mobile terminal or an IrDA mobile terminal or a mobile terminal through a cable.

44. (Currently Amended) The system according to claim 39, wherein said at least one computer system comprises a personal computer or a notebook or a laptop or a PDA, or a smart phone.

45. (Previously Presented) A communication network comprising a system according to claim 39.

46. (Previously Presented) A computer readable medium encoded with a computer program product loadable into a memory of at least one computer, the computer program product comprising software code portions for performing the method of claim 24.